IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH

CENTRAL DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. ROBERT G. LUSTYIK, JR., MICHAEL L. TAYLOR, and JOHANNES W. THALER, Defendants.	AMENDED CIPA PROTECTIVE ORDER [CORRECTED][1] Case No. 2:12-CR-645-TC-DPB

This matter comes before the Court upon the United States' Motion for Reconsideration of Court's Ruling on Protective Order [Dock. No. 323]. After consideration of the United States' Motion, the Objections filed by Defendants, the United States' Reply, the classified declarations reviewed by the Court *ex parte* and under seal, and the motions hearing held on August 14, 2013, the United States' Motion is **GRANTED**, and this Amended CIPA Protective Order shall replace and supersede the prior order entered [Dock. No. 315], and govern the production and handling of classified material in this case.

This Amended CIPA Protective Order is entered in order to prevent the unauthorized disclosure or dissemination of classified national security documents and information which will

[1] The Amended CIPA Protective Order is corrected to fix a clerical error. The last line of the original Amended CIPA Protective Order (Docket No. 411) contained an incorrect cross-reference to "paragraph 20(f) above." The cross-reference should have said "paragraph 18(f) above." That clerical change is the only difference between the original and this corrected order. No substantive change has been made to the August 23, 2013 order.

be reviewed by, or made available to, or are otherwise known by or in the possession of, any of the defendants and defense counsel in this case.

Pursuant to the authority granted under Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. III (CIPA); the Security Procedures Established Pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA Section 9; hereinafter "Security Procedures"); Rules 16(d) and 57 of the Federal Rules of Criminal Procedure; the general supervisory authority of the Court; and in order to protect the national security, it is hereby

ORDERED that:

1. The Court finds that this case will involve classified national security documents and information, the storage, handling, and control of which, by law or regulation, requires special security precautions, and access to which requires a security clearance and a “need-to-know.”

2. The purpose of this Order is to establish the procedures that must be followed by the defendants, all defense counsel of record, their designated employees, and other counsel involved in this case, translators for the defense, and all other individuals who receive access to, or otherwise are in possession of, classified documents or information in connection with this case.

3. The procedures set forth in this Amended CIPA Protective Order and CIPA shall apply to all pre-trial, trial, post-trial, and appellate aspects of this case, and may be modified from time to time by further order of the Court acting under Fed. R. Crim. P. 16(d); Sections 3 and 9 of CIPA; and the Court’s inherent supervisory authority to ensure a fair and expeditious trial.

Definitions

4. As used herein, the terms "classified national security documents and information," "classified documents," "classified document" and "classified information" (hereinafter, collectively, "classified information") refer to:

a. Any classified information which has been classified by any Executive Branch agency in the interests of national security or pursuant to Executive Order 13526 or its predecessor Orders as "CONFIDENTIAL," "SECRET," or "TOP SECRET," or additionally controlled as "SENSITIVE COMPARTMENTALIZED INFORMATION (SCI);" and

b. Any information regardless of its physical form or characteristics which has been derived from classified information since the date of the original indictment in this case.

5. The words "documents" or "information" shall include all written or printed matter of any kind, formal or informal, including originals, conforming copies, and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), and further include:

a. papers, correspondence, memoranda, notes, letters, reports, summaries, inter-office and intra-office communications, notations of any sort concerning conversations, meetings, or other communications, bulletins, cables, telexes, telecopies, teletypes, telegrams, telefacsimiles, emails, text messages, transcripts, invoices, accountings, worksheets, messages, and drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;

b. graphic or oral records or representations of any kind, including photographs, maps, charts, graphs, microfiche, microfilm, videotapes, sound recordings of any kind, and motion pictures;

c. electronic, mechanical, electric, magnetic, digital, or optical records of any kind, including audio tapes, video tapes, thumb drives, hard drives (both internal and external), CD-ROMs, DVD-ROMs, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes or disks, and all manner of electronic data processing storage; and,

d. information acquired orally or verbally.

6. "Access to classified information" means having access to, reviewing, reading, learning, or otherwise coming to know in any manner any classified information.

7. "Secure Area" shall mean a sensitive compartmentalized information facility (SCIF) accredited by a Classified Information Security Officer (CISO) for the storage, handling, and control of classified information, or other Secure Area so approved by the CISO.

8. All classified documents, and information contained therein, shall remain classified unless the documents bear a clear indication they have been declassified by the agency or department that is the originating agency of the document or the information contained therein ("originating agency").

9. Information in the public domain is ordinarily not classified. However, if classified information is reported in the press or otherwise enters the public domain, the information does not lose its classified status merely because it is in the public domain. Information reported in the press or otherwise in the public domain may be considered classified and subject to the provisions of CIPA if the information in fact remains classified and is confirmed by any person who has, or had, such access to classified information. Accordingly, any attempt by the defense to have classified information that has been reported in the public domain confirmed or denied at trial or in any public proceeding in this case shall be governed by CIPA and all provisions of this Order.

10. Classified Information Security Officer - In accordance with the provisions of CIPA and the Security Procedures, the Court designates Branden Forsgren as the Classified Information Security Officer (CISO) for this case, and Jennifer Campbell, Christine Gunning, Daniel Hartenstine, Joan Kennedy, Michael Macisso, Maura Peterson, Carli Rodriguez-Feo, Harry Rucker and Winfield Slade as Alternate CISOs, for the purpose of providing security arrangements necessary to protect from unauthorized disclosure any classified information that will be made available to the defendants or defense counsel in connection with this case. Defense counsel shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of all classified information.

11. Government Attorneys - The Court has been advised that the following government attorneys working on this case, United States Department of Justice (DOJ) Attorneys Peter M. Koski, John De Pue, Maria N. Lerner, Peter Mason, Anne Marie Blaylock Bacon, and their respective supervisors, have the requisite security clearances to have access to the classified information that relates to this case. All references to government attorneys, or attorneys for the government, as used in this Order refer only to the attorneys listed in this paragraph and their respective supervisors.

12. Protection of Classified Information - The Court finds that, in order to protect the classified information involved in this case, no person shall have access to the classified information in this case without an appropriate security clearance, as described in more detail below, including the defendants, defense counsel, defense counsel employees (including translators), and any witness for the defense. No defense counsel or defense counsel employee, including any translator, shall have access to any classified information in this case unless that person shall also have signed the Amended Memorandum of Understanding (Amended MoU) in

the form attached hereto, agreeing to comply with the terms of this Order. The signed Amended MoU shall be filed with the Court. The substitution, departure, or removal for any reason from this case of counsel for any defendant, or anyone associated with the defense as an employee or otherwise, shall not release that person from the provisions of this Order or the Amended MoU executed in connection with this Order.

Persons other than government attorneys, appropriately cleared DOJ employees, and personnel of the originating agency, can only obtain access to classified information after having been granted a security clearance by the DOJ through the CISO, granted access by the appropriate government agency, and with the permission of the Court, either through this Order (for those named in paragraph 13 below), or by separate Order upon a showing of a need to know. Before any person other than government attorneys, appropriately cleared DOJ employees, and personnel of the originating agency, is permitted by the Court to inspect and review classified information, that person must also sign the Amended MoU.

13. Defense Counsel - Subject to the provisions of paragraph 12, the following attorneys for the defense, their approved co-workers, and their translator(s) (collectively, "the defense" or "defense counsel") may be given access to classified information as required by the government's discovery obligations and otherwise as necessary to prepare for proceedings in this case: Raymond Mansolillo, Nathan Crane, J. Michael Hansen, Daniel Marino, Tillman Finley, Rebecca Skordas, Daniel Calabro, and Darin Goff.

The court is aware that Defendant Lustyik signed nondisclosure agreements as part of his former employment as an FBI agent. Those agreements went into effect before Mr. Lustyik was indicted in this case. Nothing in this Order shall be construed as a limitation on the government's ability to enforce those agreements.

Any additional person whose assistance the defense reasonably requires may only have access to classified information in this case after obtaining from the Court -- with prior notice to the United States -- an approval for access to the appropriate level of classification on a need-to-know basis, and after satisfying the other requirements described in this Order for access to classified information. The substitution, departure or removal from this case of defense counsel or any other cleared person associated with the defense as an employee or witness or otherwise, shall not release that person from the provisions of this Order, the Amended MoU, or any additional non-disclosure agreements executed in connection with this Order.

14. Area of Review - The CISO shall arrange for an appropriately approved Secure Area for use by the defense. The CISO shall, in consultation with the United States Marshals Service, establish procedures to assure that the Secure Area is accessible to the defense during normal business hours, after hours, and on weekends. The Secure Area shall contain a separate working area for the defense and will be outfitted with any secure office equipment requested by the defense that is reasonable and necessary to the preparation of the defendants' defense in this case. The CISO, in consultation with defense counsel, shall establish procedures to assure that the Secure Area is maintained and operated in the most efficient manner consistent with the protection of classified information and the needs of the defense. No documents containing classified information may be removed from this Secure Area unless authorized by the CISO. The CISO shall not reveal to the United States the content of any conversations he may hear among the defense, nor reveal the nature of documents being reviewed by them, or the work generated by them. In addition, the presence of the CISO shall not operate as a waiver of, limitation on, or otherwise render inapplicable, the attorney-client privilege.

15. Filings with the Court - Until further order of this Court, any pleading or other document filed by the defense that it reasonably expects may contain classified information shall be filed under seal with the Court through the CISO, or his designee, by 4 p.m. on the day of filing, and shall be marked, "Filed In Camera and Under Seal with the Classified Information Security Officer." The date and time of physical submission to the CISO or his designee shall be considered the date and time of filing. At the time of making a submission to the CISO or his designee, defense counsel shall file on the public record in the CM/ECF system a "Notice of Filing" notifying the Court that the submission was made and providing a title of the document. The title may not disclose any potentially classified information.

The CISO shall promptly examine the pleading or document and, in consultation with representatives of the appropriate agencies, determine whether the pleading or document contains classified information. If the CISO determines that the pleading or document contains classified information, he shall ensure that that portion of the pleading or document, and only that portion, is marked with appropriate classification marking and that the pleading or document remains under seal. The CISO or his designee shall immediately deliver under seal to the Court and counsel for the United States (unless such filing is ex parte) any pleading or document filed by the defense that contains classified information.

If the CISO determines that some or all of the pleading or document does not contain classified information, he shall immediately provide notice to counsel for the filing party of those specific portions of the pleading or document which the CISO has determined do not contain such information and may be unsealed and placed in the public record so far as the CISO is concerned. The filing party shall have three (3) business days from receipt of such notice to file a motion with the Court seeking leave for the pleading or document, or a specified portion thereof,

to be filed under seal. Upon notice of the filing of such a motion, the CISO and/or his designee shall refrain from placing the document or pleading on the public record until such time as the Court rules on the motion, after which the document or pleading shall be docketed as the Court directs.

16. Any pleading or other document filed by the United States containing classified information shall be filed under seal with the Court through the CISO or his designee. The date and time of physical submission to the CISO or his designee shall be considered the date and time of filing and should occur no later than 4 p.m. The CISO or his designee shall immediately deliver under seal to the Court and counsel for the defense (unless such filing is ex parte) any pleading or document filed by the government that contains classified information.

17. The CISO shall maintain a separate sealed record for those materials which are classified. The CISO shall be responsible for also maintaining the secured records for purposes of later proceedings or appeal.

18. Access to Classified Information - In the interest of national security, the defendants may be excluded from access to classified information. Cleared defense counsel, their designated employees, and translators, shall have access to classified information only as follows:

a. All classified information produced by the United States to the defense, in discovery or otherwise, and all classified information possessed, created, or maintained by the defense, shall be stored, maintained, and used only in the Secure Area established by the CISO, unless otherwise authorized by the CISO;

b. Cleared defense counsel shall have free access to the classified information made available to them in the Secure Area, and shall be allowed to take notes and

prepare documents with respect to those materials. However, the cleared defense counsel shall not, except under separate Court order, disclose the classified information, either directly, indirectly, or in any manner which would disclose the existence of such, to pursue leads or in the defense of the defendant;

c. No person, including the defense, shall copy or reproduce any classified information in any form, except with the approval of the CISO or in accordance with the procedures established by the CISO for the operation of the Secure Area;

d. All documents prepared by the defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information, shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information, and in the Secure Area on approved word processing equipment and in accordance with the procedures approved by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, and exhibits) containing classified information shall be maintained in the Secure Area unless the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the United States;

e. The defense shall discuss classified information only within the Secure Area authorized by the CISO, and shall not discuss or attempt to discuss classified information over any standard commercial telephone instrument or office intercommunication system, including the Internet;

f. The defense shall not disclose, without prior approval by the United States in the first instance or by the Court upon notice to and opportunity to be heard by the United

States, the contents of any classified information to any person not authorized pursuant to this Order, including the defendants and defense witnesses, except the Court, Court personnel, and the attorneys for the United States, who have been identified by the CISO as having the appropriate clearances and the need to know that information. Counsel for the United States shall be given notice of and an opportunity to be heard by the Court for disclosure to a person not named in this Order. Any person approved by the United States in the first instance, or by the Court upon notice to and an opportunity to be heard by the United States for disclosure under this paragraph, shall be required to obtain the appropriate security clearance as necessary, to sign and submit to the Court the Amended MoU appended to this Order, and to comply with all terms and conditions of this Order. If preparation of the defense requires that classified information be disclosed to persons not named in this Order, then, upon approval by the United States in the first instance, or by the Court upon notice to and an opportunity to be heard by the United States, the CISO shall promptly seek to obtain security clearances for them at the request of defense counsel.

19. Procedures for the use or the public disclosure of classified information by the defense shall be those provided in Sections 5 and 6 of CIPA. No classified information may be used or disclosed by the defense except:

a. To the Court, Court personnel, and government attorneys and their agents and employees identified by the CISO as holding proper approvals for access to classified information;

b. In accordance with the procedures of CIPA and the procedures established by the CISO;

c. To persons who have been authorized to have access to classified information pursuant to this Order or to CIPA; and,

d. To representatives of the agency or department originating the classified information, who have been identified by the CISO as holding appropriate security clearances and having the need to know the classified information.

To facilitate the defense filing of notices required under Section 5 of CIPA, the CISO shall make arrangements with the appropriate agencies for a determination of the classification level, if any, of materials or information either within the possession of the defense or about which the defense has knowledge and which the defense intends to use in any way at any pretrial proceeding, deposition, or trial. Nothing submitted by the defense to the CISO pursuant to this paragraph shall be made available to counsel for the United States unless so ordered by the Court, or so designated by the defense. Any and all items which are classified shall be listed in the defendant's Section 5 notice.

20. Violations of this Order - Any unauthorized disclosure or dissemination of classified information may constitute violations of United States criminal laws. In addition, any violation of the terms of this Order shall be immediately brought to the attention of the Court and may result in a charge of contempt of the Court and possible referral for criminal prosecution. Any breach of this Order may also result in the termination of a person's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized use, disclosure, retention, or negligent handling of classified information could cause serious damage, and in some cases exceptionally grave damage, to the national security of the United States. Persons subject to this Order are also advised that such disclosure may be used to the advantage of a foreign nation or against the interests of the United States, regardless of whether the foreign

nation is considered a friend or enemy of the United States. This Order is intended to ensure that those authorized by the Order to receive classified information will never divulge the classified information disclosed to them in connection with this case to anyone who is not now authorized to receive it, or otherwise use the classified information, without prior written authorization from the originating agency and in conformity with this Order.

21. All classified information to which defense counsel and defense counsel employees, including translators, have access in this case are now and will remain the property of the United States. The defense counsel and defense counsel employees, including translators, who receive classified information shall return all such classified information in their possession obtained through discovery from the United States in this case, or for which they are responsible because of access to classified information, upon demand of the CISO. The notes, summaries, and other documents prepared by the defense that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of this case. At the conclusion of this case, all such notes, summaries, or other documents are to be destroyed by the CISO in the presence of defense counsel, if so desired.

22. Nothing in this Order shall preclude the United States from seeking a further protective order pursuant to Rule 16(d) as to particular items of discovery material.

23. A copy of this Order shall be issued forthwith to counsel for the defendants, who shall be responsible for advising the defendants and defense counsel employees, including translators, of the contents of this Order. The defense counsel and defense counsel employees to be provided access to classified information shall execute the Amended MoU appended to this Order, and defense counsel shall file executed originals of such document upon the United States. The execution and filing of the Amended MoU is a condition precedent for defense

counsel, defense counsel employees, and any other person working for the defense to have access to classified information. It is also a condition precedent for the defendant and any defense witness to have access to classified information pursuant to paragraph 18(f) above.

DATED this 28th day of August, 2013.

BY THE COURT:

Tena Campbell

TENA CAMPBELL
U.S. District Judge

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH

CENTRAL DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. ROBERT G. LUSTYIK, JR., MICHAEL L. TAYLOR, and JOHANNES W. THALER, Defendants.	AMENDED MEMORANDUM OF UNDERSTANDING FOR AMENDED CIPA PROTECTIVE ORDER Case No. 2:12-CR-645-TC-DPB

1. Having familiarized myself with the Amended CIPA Protective Order entered by the Court, I understand that I have already received and/or may be the future recipient of documents and information which pertain to the national security of the United States of America and which are the property of the United States, and that such documents and information, together with the methods of collection of such, are classified according to security standards set by the United States government.

2. I agree that I shall never divulge, publish, or reveal, either by word, conduct, or any other means, such classified documents or information unless specifically authorized in writing to do so by an authorized representative of the United States government, or as authorized by the Court pursuant to the Classified Information Procedures Act (CIPA) or the Amended CIPA Protective Order entered in the above-captioned case, or as otherwise ordered by the Court.

3. I agree that this Amended Memorandum of Understanding and any other nondisclosure agreement signed by me in connection with this case will remain forever binding upon me.

4. I have received, read, and understand the Amended CIPA Protective Order entered by the United States District Court for the District of Utah in the above-captioned case, and I agree to comply with the provisions contained therein.

5. I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief.

Name: _____

Date and
Place of Birth: _____

_____
(Signature)

_____
Date